

# Contents

To the Student	xv
How to Read a Mathematics Book	xvi
Exercises	xvii
To the Instructor	xix
Audience and Prerequisites	xix
Topics Covered and Navigating the Sections	xix
Sample Course Outlines	xxi
Special Features	xxi
What's New in This Second Edition	xxiii
Acknowledgments	xxv
This New Edition	xxv
From the First Edition	xxv

---

<b>1</b>	<b>Fundamentals</b>	<b>1</b>
1	Joy	1
Why?	1	
The Agony and the Ecstasy	2	
Exercise	2	
2	Definition	2
Recap	5	
Exercises	5	
3	Theorem	8
The Nature of Truth	8	
If-Then	9	
If and Only If	11	
And, Or, and Not	12	
What Theorems Are Called	13	
Vacuous Truth	14	
Recap	14	
Exercises	15	
4	Proof	16
A More Involved Proof	20	
Proving If-and-Only-If Theorems	22	

	Proving Equations and Inequalities	24
	Recap	25
	Exercises	25
<b>5</b>	<b>Counterexample</b>	<b>25</b>
	Recap	27
	Exercises	27
<b>6</b>	<b>Boolean Algebra</b>	<b>27</b>
	More Operations	31
	Recap	32
	Exercises	32
	<b>Chapter 1 Self Test</b>	<b>34</b>

---

<b>2</b>	<b>Collections</b>	<b>37</b>
<b>7</b>	<b>Lists</b>	<b>37</b>
	Counting Two-Element Lists	37
	Longer Lists	40
	Recap	43
	Exercises	43
<b>8</b>	<b>Factorial</b>	<b>45</b>
	Much Ado About 0!	46
	Product Notation	47
	Recap	48
	Exercises	48
<b>9</b>	<b>Sets I: Introduction, Subsets</b>	<b>49</b>
	Equality of Sets	51
	Subset	53
	Counting Subsets	55
	Power Set	57
	Recap	57
	Exercises	57
<b>10</b>	<b>Quantifiers</b>	<b>58</b>
	There Is	58
	For All	59
	Negating Quantified Statements	60
	Combining Quantifiers	61
	Recap	62
	Exercises	63
<b>11</b>	<b>Sets II: Operations</b>	<b>64</b>
	Union and Intersection	64
	The Size of a Union	66
	Difference and Symmetric Difference	68

Cartesian Product	73
Recap	74
Exercises	74
<b>12 Combinatorial Proof: Two Examples</b>	<b>76</b>
Recap	80
Exercises	80
<b>Chapter 2 Self Test</b>	<b>80</b>

---

### **3 Counting and Relations 83**

<b>13 Relations 83</b>	
Properties of Relations	86
Recap	87
Exercises	87
<b>14 Equivalence Relations 89</b>	
Equivalence Classes	92
Recap	95
Exercises	96
<b>15 Partitions 98</b>	
Counting Classes/Parts	100
Recap	102
Exercises	102
<b>16 Binomial Coefficients 104</b>	
Calculating $\binom{n}{k}$	107
Pascal's Triangle	109
A Formula for $\binom{n}{k}$	111
Recap	113
Exercises	113
<b>17 Counting Multisets 117</b>	
Multisets	117
Formulas for $\binom{n}{k}$	119
Recap	122
Exercises	122
<b>18 Inclusion-Exclusion 123</b>	
How to Use Inclusion-Exclusion	126
Derangements	129
A Ghastly Formula	132
Recap	132
Exercises	132
<b>Chapter 3 Self Test 133</b>	

---

<b>4</b>	<b>More Proof</b>	<b>135</b>
19	Contradiction	135
	Proof by Contrapositive	135
	Reductio ad Absurdum	137
	A Matter of Style	141
	Recap	141
	Exercises	141
20	Smallest Counterexample	142
	Well-Ordering	148
	Recap	153
	Exercises	153
	And Finally	154
21	Induction	155
	The Induction Machine	155
	Theoretical Underpinnings	157
	Proof by Induction	157
	Proving Equations and Inequalities	160
	Other Examples	162
	Strong Induction	163
	A More Complicated Example	165
	A Matter of Style	168
	Recap	168
	Exercises	168
22	Recurrence Relations	171
	First-Order Recurrence Relations	172
	Second-Order Recurrence Relations	175
	The Case of the Repeated Root	178
	Sequences Generated by Polynomials	180
	Recap	187
	Exercises	188
	Chapter 4 Self Test	190

---

<b>5</b>	<b>Functions</b>	<b>193</b>
23	Functions	193
	Domain and Image	195
	Pictures of Functions	196
	Counting Functions	197
	Inverse Functions	198
	Counting Functions, Again	202
	Recap	203
	Exercises	203

<b>24</b>	<b>The Pigeonhole Principle</b>	<b>205</b>
	Cantor's Theorem	208
	Recap	210
	Exercises	210
<b>25</b>	<b>Composition</b>	<b>211</b>
	Identity Function	214
	Recap	215
	Exercises	215
<b>26</b>	<b>Permutations</b>	<b>216</b>
	Cycle Notation	217
	Calculations with Permutations	220
	Transpositions	221
	A Graphical Approach	226
	Recap	228
	Exercises	228
<b>27</b>	<b>Symmetry</b>	<b>231</b>
	Symmetries of a Square	231
	Symmetries as Permutations	232
	Combining Symmetries	233
	Formal Definition of Symmetry	235
	Recap	236
	Exercises	236
<b>28</b>	<b>Assorted Notation</b>	<b>236</b>
	Big oh	236
	$\Omega$ and $\Theta$	239
	Little oh	240
	Floor and Ceiling	241
	Recap	242
	Exercises	242
	<b>Chapter 5 Self Test</b>	<b>242</b>

---

## **6 Probability 245**

<b>29</b>	<b>Sample Space</b>	<b>245</b>
	Recap	248
	Exercises	248
<b>30</b>	<b>Events</b>	<b>249</b>
	Combining Events	252
	The Birthday Problem	253
	Recap	254
	Exercises	255

<b>31</b>	<b>Conditional Probability and Independence</b>	<b>257</b>
	Independence	259
	Independent Repeated Trials	261
	The Monty Hall Problem	262
	Recap	263
	Exercises	263
<b>32</b>	<b>Random Variables</b>	<b>266</b>
	Random Variables as Events	267
	Independent Random Variables	269
	Recap	270
	Exercises	270
<b>33</b>	<b>Expectation</b>	<b>271</b>
	Linearity of Expectation	276
	Product of Random Variables	279
	Expected Value as a Measure of Centrality	282
	Variance	283
	Recap	287
	Exercises	287
	<b>Chapter 6 Self Test</b>	<b>289</b>

---

<b>7</b>	<b>Number Theory</b>	<b>293</b>
<b>34</b>	<b>Dividing</b>	<b>293</b>
	Div and Mod	296
	Recap	297
	Exercises	297
<b>35</b>	<b>Greatest Common Divisor</b>	<b>298</b>
	Calculating the gcd	299
	Correctness	301
	How Fast?	302
	An Important Theorem	304
	Recap	307
	Exercises	307
<b>36</b>	<b>Modular Arithmetic</b>	<b>309</b>
	A New Context for Basic Operations	309
	Modular Addition and Multiplication	310
	Modular Subtraction	311
	Modular Division	313
	A Note on Notation	318
	Recap	318
	Exercises	318

**37 The Chinese Remainder Theorem 320**

Solving One Equation	320
Solving Two Equations	322
Recap	324
Exercises	324

**38 Factoring 325**

Infinitely Many Primes	327
A Formula for Greatest Common Divisor	328
Irrationality of $\sqrt{2}$	329
Recap	331
Exercises	331

**Chapter 7 Self Test 335****8 Algebra 337****39 Groups 337**

Operations	337
Properties of Operations	338
Groups	340
Examples	342
Recap	345
Exercises	345

**40 Group Isomorphism 347**

The Same?	347
Cyclic Groups	349
Recap	352
Exercises	352

**41 Subgroups 353**

Lagrange's Theorem	356
Recap	359
Exercises	359

**42 Fermat's Little Theorem 362**

First Proof	362
Second Proof	363
Third Proof	366
Euler's Theorem	367
Primality Testing	368
Recap	369
Exercises	369

**43 Public Key Cryptography I: Introduction 370**

The Problem: Private Communication in Public	370
Factoring	370

Words to Numbers	371
Cryptography and the Law	373
Recap	373
Exercises	373
<b>44 Public Key Cryptography II: Rabin's Method</b>	<b>373</b>
Square Roots Modulo $n$	374
The Encryption and Decryption Procedures	378
Recap	379
Exercises	379
<b>45 Public Key Cryptography III: RSA</b>	<b>380</b>
The RSA Encryption and Decryption Functions	381
Security	383
Recap	384
Exercises	384
<b>Chapter 8 Self Test</b>	<b>385</b>

## **9 Graphs 389**

<b>46 Fundamentals of Graph Theory</b>	<b>389</b>
Map Coloring	389
Three Utilities	391
Seven Bridges	391
What Is a Graph?	392
Adjacency	393
A Matter of Degree	394
Further Notation and Vocabulary	396
Recap	397
Exercises	397
<b>47 Subgraphs</b>	<b>399</b>
Induced and Spanning Subgraphs	400
Cliques and Independent Sets	402
Complements	403
Recap	404
Exercises	404
<b>48 Connection</b>	<b>406</b>
Walks	406
Paths	407
Disconnection	410
Recap	411
Exercises	411
<b>49 Trees</b>	<b>413</b>
Cycles	413
Forests and Trees	413

	Properties of Trees	414
	Leaves	416
	Spanning Trees	418
	Recap	419
	Exercises	420
<b>50</b>	<b>Eulerian Graphs</b>	<b>421</b>
	Necessary Conditions	422
	Main Theorems	423
	Unfinished Business	425
	Recap	426
	Exercises	426
<b>51</b>	<b>Coloring</b>	<b>427</b>
	Core Concepts	427
	Bipartite Graphs	429
	The Ease of Two-Coloring and the Difficulty of Three-Coloring	433
	Recap	434
	Exercises	434
<b>52</b>	<b>Planar Graphs</b>	<b>435</b>
	Dangerous Curves	435
	Embedding	436
	Euler's Formula	437
	Nonplanar Graphs	440
	Coloring Planar Graphs	442
	Recap	444
	Exercises	444
	<b>Chapter 9 Self Test</b>	<b>446</b>
<hr/>		
<b>10</b>	<b>Partially Ordered Sets</b>	<b>449</b>
<b>53</b>	<b>Fundamentals of Partially Ordered Sets</b>	<b>449</b>
	What Is a Poset?	449
	Notation and Language	452
	Recap	454
	Exercises	454
<b>54</b>	<b>Max and Min</b>	<b>455</b>
	Recap	457
	Exercises	457
<b>55</b>	<b>Linear Orders</b>	<b>458</b>
	Recap	460
	Exercises	461

<b>56</b>	<b>Linear Extensions</b>	<b>461</b>
	Sorting	465
	Linear Extensions of Infinite Posets	467
	Recap	468
	Exercises	468
<b>57</b>	<b>Dimension</b>	<b>469</b>
	Realizers	469
	Dimension	471
	Embedding	473
	Recap	476
	Exercises	476
<b>58</b>	<b>Lattices</b>	<b>477</b>
	Meet and Join	477
	Lattices	479
	Recap	481
	Exercises	482
	<b>Chapter 10 Self Test</b>	<b>483</b>

---

## **Appendices 487**

<b>A</b>	<b>Lots of Hints and Comments; Some Answers</b>	<b>487</b>
<b>B</b>	<b>Solutions to Self Tests</b>	<b>515</b>
	Chapter 1	515
	Chapter 2	516
	Chapter 3	518
	Chapter 4	520
	Chapter 5	524
	Chapter 6	526
	Chapter 7	530
	Chapter 8	532
	Chapter 9	535
	Chapter 10	539
<b>C</b>	<b>Glossary</b>	<b>544</b>
<b>D</b>	<b>Fundamentals</b>	<b>552</b>
	Numbers	552
	Operations	552
	Ordering	553
	Complex Numbers	553
	Substitution	553

## **Index 555**